



SOLARWINDS®

Secure Software Development Practices and Integrating Transparency into the Software Supply Chain

Tim Brown

CISO SolarWinds



A Little History...



- SUNBURST Dec 2020 brings supply chain security into focus
- As SolarWinds responded, a high-level government official asked us a series of questions:
 - What is your approach to the secure development lifecycle?
 - How do you secure software code and its associated infrastructure?
 - What are your internal processes to validate product changes?
 - Have you implemented enterprise risk management (ERM)?
 - What are your notification procedures if a security vulnerability is discovered?
 - What internal processes are used to identify insider threats to software products?
 - What are your internal processes for screening potential employees for insider threats?
- These questions have shaped Cybersecurity and Infrastructure Security Agency (CISA) requirements and executive orders (EOs)

Software Supply Chain Security Continues to Evolve



- 'Little' supply chain: individual software products, components within the products, and vulnerabilities in those components
- 'Big' supply chain: systems made from products for a larger purpose
- EOs and Frameworks 2021–2025:
 - EO 14028 Improving the Nation's Cyber Security–May 2021
 - Software Bill of Materials (SBOM) initiatives and requirements
 - Secure Software Development Framework (SSDF)–NIST 800-218
 - Enduring Security Framework (ESF)–Securing the Software Supply Chain: Recommended Practices for Developers
 - CISA Secure Software Development Self-Attestation–Required by end of 2023
 - EO 14144 Strengthening and Promoting Innovation in the Nation's Cybersecurity–January 2025

Next Gen Build System and Transparency



- Started with 2 way builds verifying source to build
- Ended with 6 Months process of updating build environments.
- Next Gen Build Environment
 - Externalize Environments
 - Everything in Code
 - Ephemeral
 - Tamper resistant
 - Assumed breach model
- Security Contacts recorded for 90% of customers
- CNA – Issue CVEs on ourselves
- Security issues consistently tracked via Jira with Security tags
- Separate tracking and reporting model for Security
- SBOM creation integrated to build environments

SolarWinds Commitment to Self-Attestation



Requirements for Self-Attestation

- Separation of build environment
- Minimize access only to those who need it
- Multi-factor authentication and conditional access across the enterprise
- Minimize dependencies, encrypt data, monitor and alert
- Automate processes and minimize human interaction
- Scan for vulnerabilities in the build process and have processes to prioritize remediation
- SBOM
- Participate in a vulnerability disclosure program
- Attest to the efficacy of the software development practices and the integrity of third-party components
- <https://www.solarwinds.com/trust-center>

SolarWinds was prepared to self-attest and uploaded its attestation the first day the repository opened

Executive Order 14144: Jan 2025



- **Machine-Readable Secure Software Development Attestations**

- Secure Development Lifecycle (SDLC) attestations
- Build environment details: summaries of tools, dependencies, and automated checks used throughout the development pipeline
- Verification logs: records of software composition analysis, static/dynamic testing, and code reviews

- **High-Level Artifacts to Validate Attestations**

- Human-readable summaries: a statement of compliance or conformance to recognized standards
- Audit certificates or independent assessments: in critical software cases, agencies may require external auditor certification to verify the accuracy of secure development attestations
- Reference to SBOMs, which serve as key validation artifacts, mapping each software component and ensuring alignment with code provenance and dependency security attestations

- **Automated Vulnerability Disclosure and Patch Management**

- Continuous scanning: vendors must run automated tools to detect security flaws
- Patch timelines: critical vulnerabilities must be fixed within an accelerated timeframes

- **Provenance and Integrity Checks**

- Cryptographically signed builds
- Code lineage evidence

- **Continuous Compliance Monitoring**

- Regular audits: agencies (or third-party assessors) will periodically review vendors
- Incident reporting: vendors must notify the relevant agency within 24 hours if any compromise occurs in the supply chain

For This Community



- Expect more from software vendors (DoDIN APL, self-attestation, SBOMs, etc.)
- Events can and have been a catalyst to change...if you participate!
- Transparency is a key to security in our supply chain
- SBOM is a good start, but the latest EO will drive vendors to additional transparency
- Our adversaries are sophisticated, patient, and thoughtful...they only need to get lucky once
- We raise the bar by working together, and we make it more difficult for our adversaries to succeed



THANK YOU



The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

